NICTER Dataset 2021

笠間 貴弘

国立研究開発法人情報通信研究機構
サイバーセキュリティ研究所 サイバーセキュリティ研究室
研究マネージャー

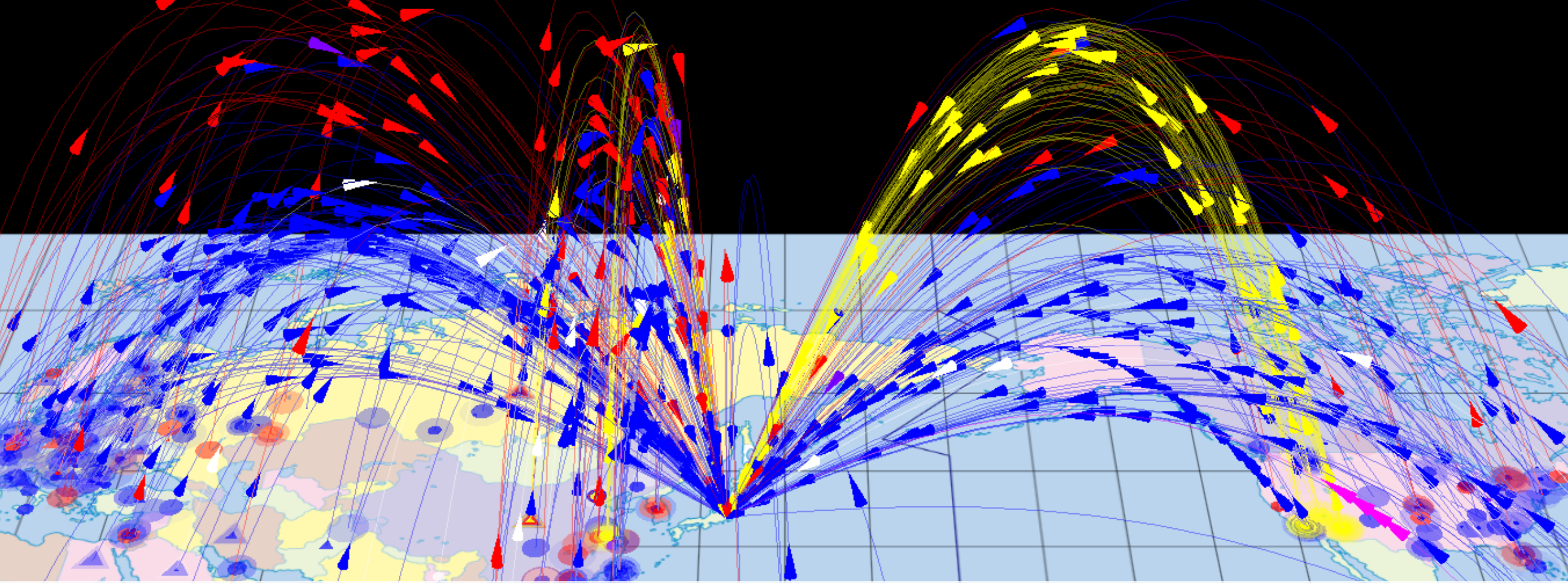
NICT National Institute of Information and Communications Technology

NICTER Network Incident analysis Center for Tactical Emergency Response

NICTER Dataset 2021

- **ダークネットトラフィックデータ**
  - ✓/20(約4千アドレス)のダークネットトラフィック
  - ✓観測期間は2011年4月1日から現在まで**10年間以上**
  - ✓NONSTOP上で提供（pcap+DB）

- **スパムメールデータ**
  - ✓NICTのメールサーバに届いたダブルバウンスメール
  - ✓観測期間は2015年1月1日から現在まで6年間以上
  - ✓NONSTOP上で提供（メールファイル）

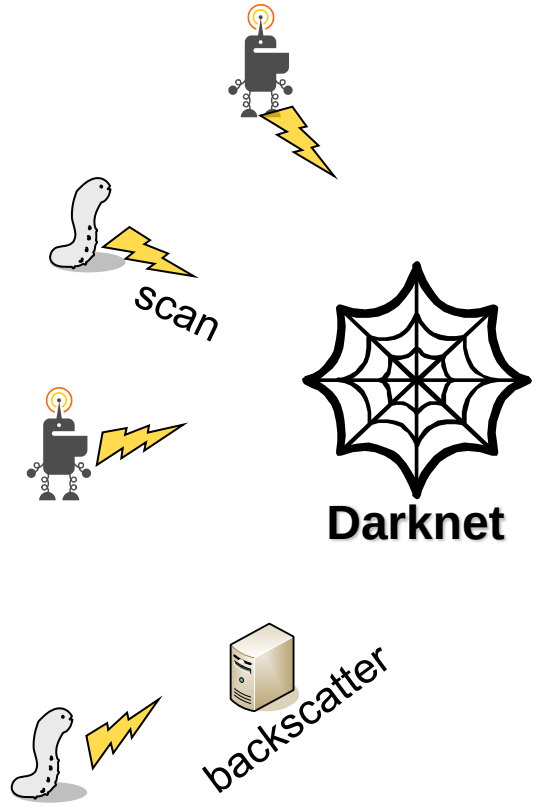


NICTER

- サイバー攻撃リアルタイム大規模観測・分析システム
- 国内外で30万の未使用IPアドレス“**ダークネット**”を観測
- 無差別型サイバー攻撃の大局的な傾向把握に有効

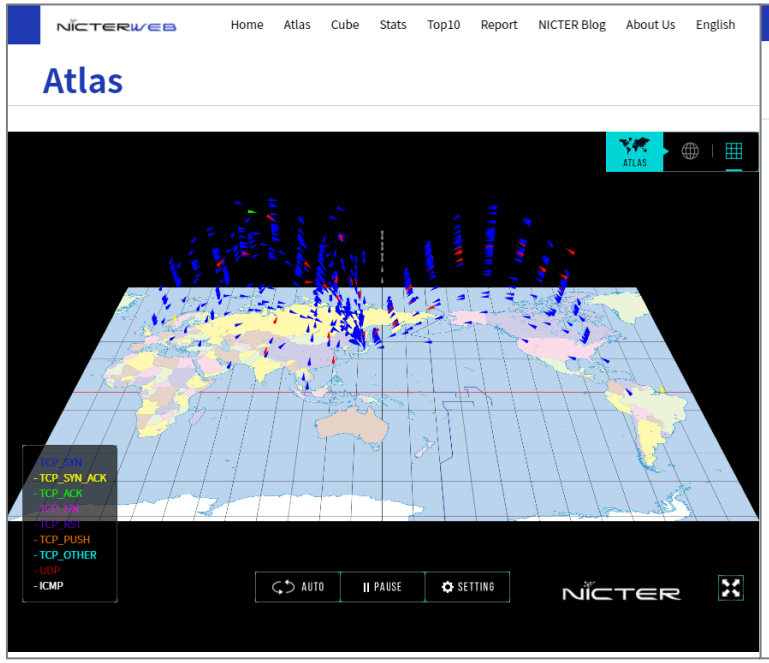
ダークネット観測とは？

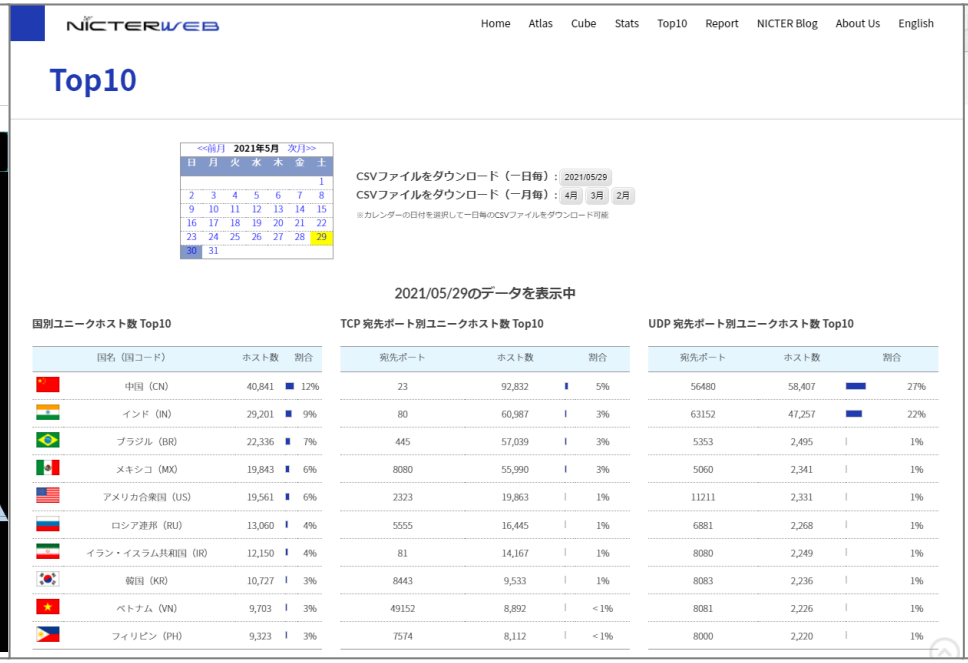
- **ダークネット：未使用のIPアドレス空間**
  - ✓正常な通信は“基本的に”届かない
- **実際は大量の通信が届く**
  - ✓ マルウェアによるスキャン
  - ✓ DDoS攻撃の跳ね返り
  - ✓ リフレクション攻撃の準備活動
  - ✓ etc.
- **ダークネットの観測によって パンデミックの兆候が分かる**
  - ✓ パンデミック：マルウェアの大量感染



観測結果や分析結果は一般公開もしています

- NICTERWEB (http://www.nicter.jp/)
- NICTER Blog (http://blog.nicter.jp)
- NICTER 観測レポート 2016~2020



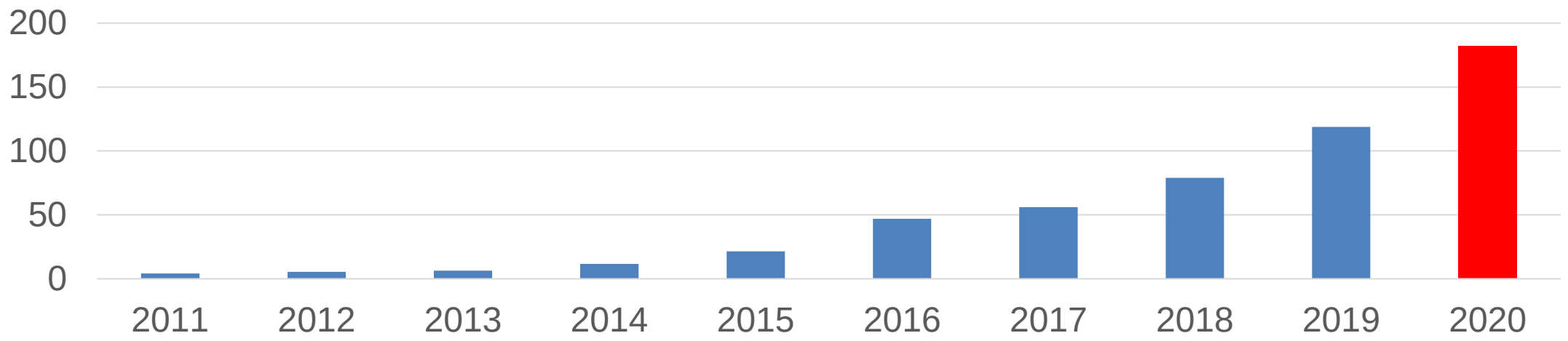


よくある誤解（その１）

Q：ワームとかもう古いしスキャンなんて飛んでこないでしょ？

A: なんかそういうデータあるんですか？

（パケット数，単位：万）

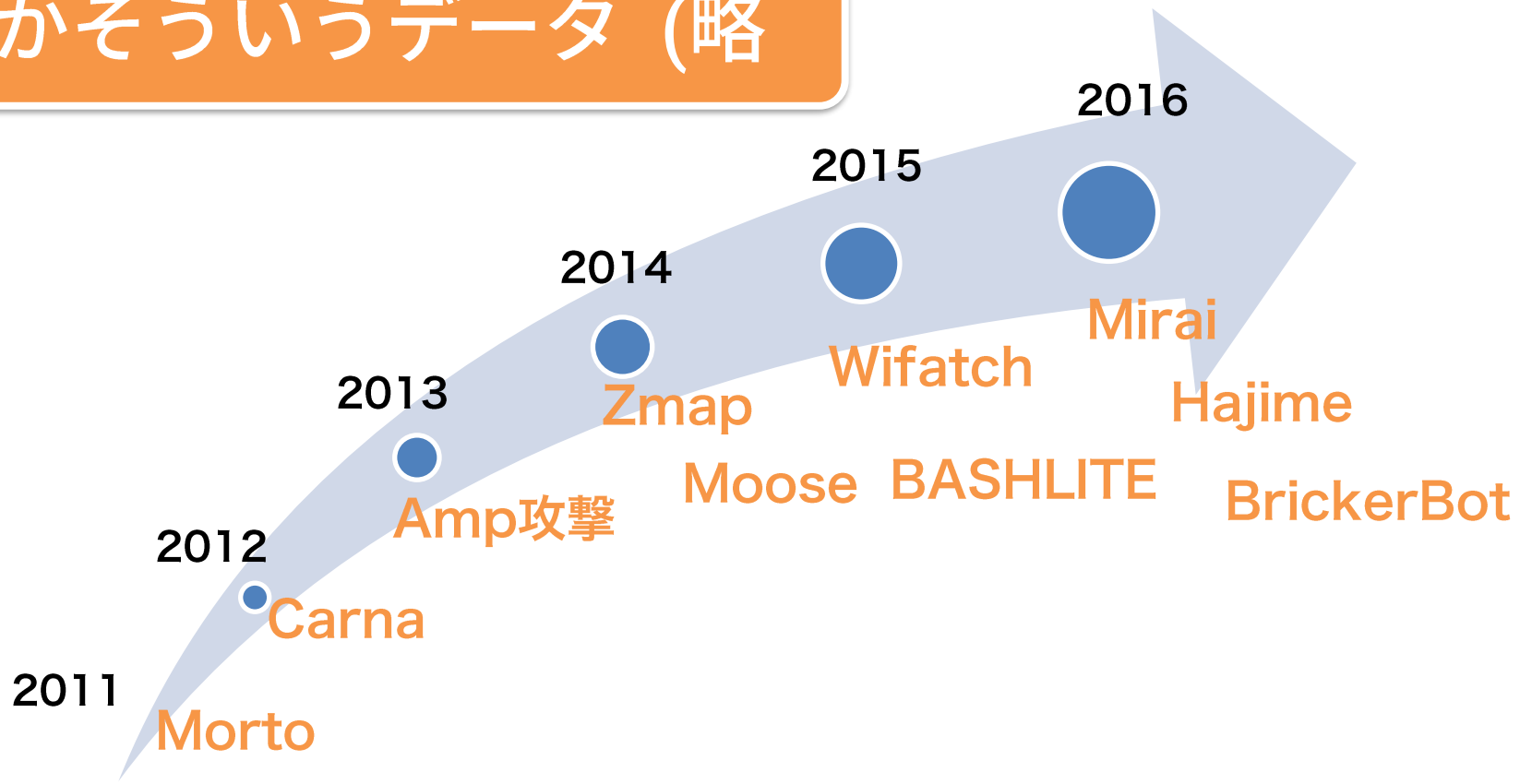


1 IPアドレスあたりの年間総観測パケット数

よくある誤解（その２）

Q：スキャンしているのなんて古いConfickerとかだけじゃないの？

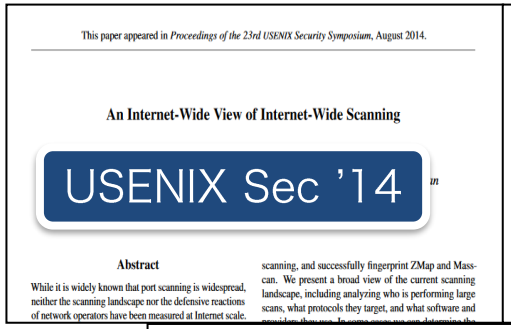
A: なんかそういうデータ（略

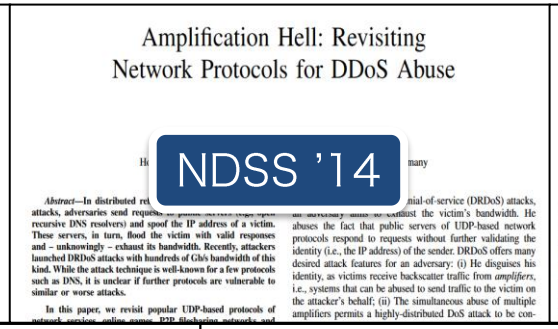


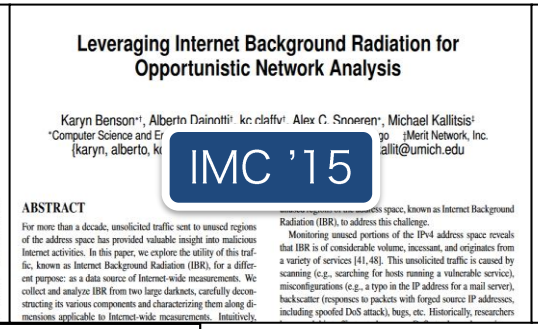
よくある誤解（その３）

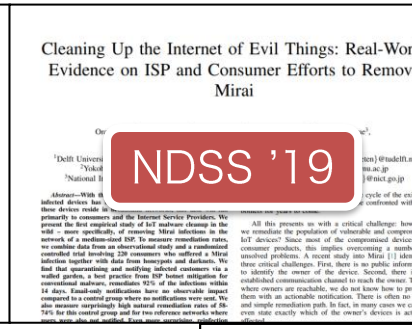
Q：今更ダークネットデータ使った論文とか出てないんじゃない？

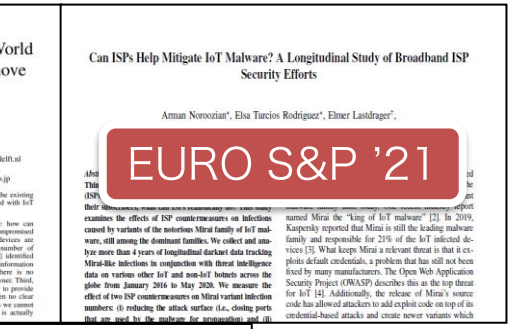
A: な（略

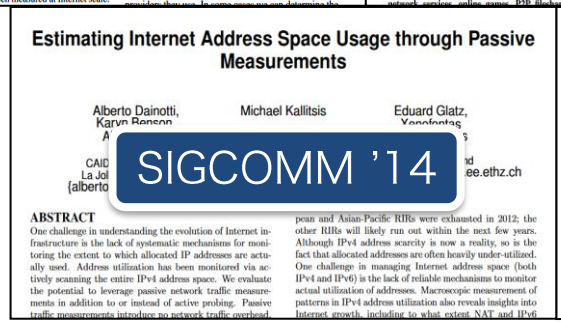


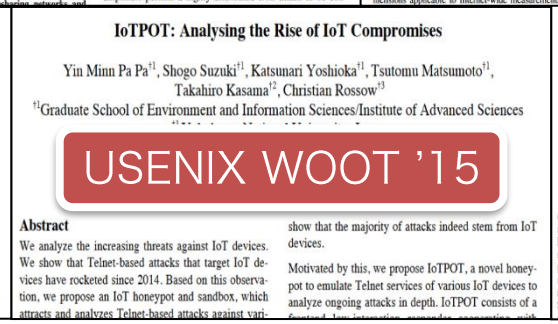


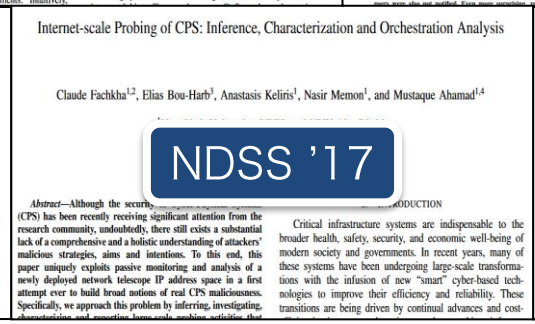


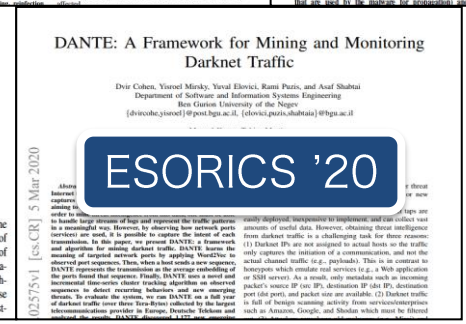










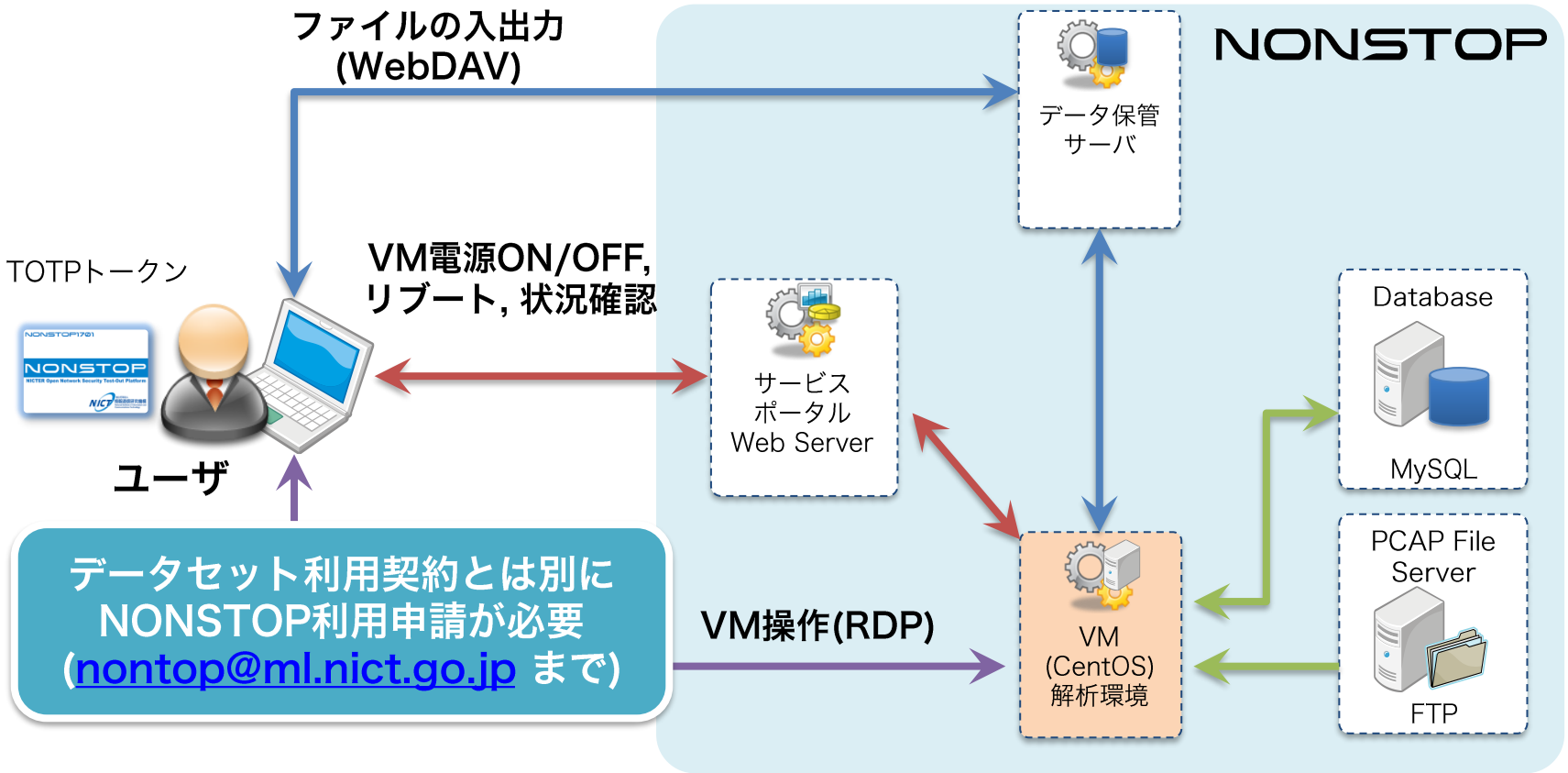


National Institute of Information and Communications Technology

Network Incident analysis Center for Tactical Emergency Response

NICTERデータセットはNONSTOP上で提供

- サイバーセキュリティ情報を遠隔から安全に利用してもらうための環境



NICTER Dataset まとめ

- **今年度提供するデータは２種類：**
  - ダークネットトラフィック
  - スパムメールデータ（要望があれば）

- **データセットはNONSTOP上で提供：**
  - データにアクセスできるVM環境をユーザ毎に用意
  - 利用申請は nonstop@ml.nict.go.jp まで（継続の方も要連絡）

- **メリット：**
  - リアルタイムかつ継続的(10年間以上)のデータセット
  - 加工されていない生データなので用途は自由